Building Your Security Team

There is some paperwork and policy writing required to improve security. Part of the process is to write down necessary tasks, who is responsible, how often the task is to be performed, and details of remediation should there be an issue. This checklist is to get started. There are more resources in the NIST documents in the next section.

1. Identity management, credentials, and access
2. Ongoing Administration
3. Risk management process
4. Responding to an security issue
5. Securing data
6. Network Security
7. System Security
8. Application Security

User Identification and Credentials

We will download and take a look at some FIPS guides. Each of these guides would take many hours to read and digest. Implementing the security improvements may take quite a while. Plan time after class to read through the documents mentioned in detail.

1. Download the FIPS 200 and 201-2 guide onto your local system. Start here: https://csrc.nist.gov/publications/fips and locate both titles.
2. Read through the table of contents of FIPS 200 then section 4 SECURITY CONTROL SELECTION. Locate the NIST SP 800-53 mentioned in the section.
3. Read the table of contents of NIST SP 800-53. Take note of total number of pages and how many pages are part of Appendix F. Skim through some of the catalog entries such as AC_4 INFORMATION FLOW ENFORCEMENT

Building Your Security Team

There is some paperwork and policy writing required to improve security. Part of the process is to write down necessary tasks, who is responsible, how often the task is to be performed, and details of remediation should there be an issue. This checklist is to get started. There are more resources in the NIST documents in the next section.

1. Identity management, credentials, and access
2. Ongoing Administration
3. Risk management process
4. Responding to an security issue
5. Securing data
6. Network Security
7. System Security
8. Application Security

User Identification and Credentials

We will download and take a look at some FIPS guides. Each of these guides would take many hours to read and digest. Implementing the security improvements may take quite a while. Plan time after class to read through the documents mentioned in detail.

- Download the FIPS 200 and 201-2 guide onto your local system. Start here: https://csrc.nist.gov/publications/fips and locate both titles.
- Read through the table of contents of FIPS 200 then section 4 SECURITY CONTROL SELECTION. Locate the NIST SP 800-53 mentioned in the section.
- Read the table of contents of NIST SP 800-53. Take note of total number of pages and how many pages are part of Appendix F. Skim through some of the catalog entries such as AC_4 INFORMATION FLOW ENFORCEMENT
- Make a plan to categorize all of your systems as low-impact, moderate-impact or high-impact information systems.
- Read through the table of contents of FIPS 201-2. Then find section 2.1 Control Objectives and understand the four control objectives and a manner to ensure that objective in your environment.

Tracking Known Issues

- View https://nvd.nist.gov/vuln/search and type in Kubernetes as the Keyword Search.
- Select a record which indicates a CRITICAL vulnerability, and read through current description and the product that it effects. Continue to read through other references, weakness enumeration, and known affected software configurations.
- Determine who in your organization will be responsible for keeping track of CVE updates. Would it be one group, or a different person in working with individual project software.

CIS Benchmarks

In this exercise we will download a free benchmark for Kubernetes from the Center for Internet Security ®. You may want to schedule a regular return for new or different information.

- Open a local browser and visit https://www.cisecurity.org/cis-benchmarks/
- Scroll to expand information on Kubernetes.
- Among the expanded list you may note that only one version is considered current. Select the current benchmark
- Fill out your contact information and accept the terms. An email will be sent to the email given in a minute or two. Inside the email is a link to Access the PDFs, which will open a website to download the freely available PDFs.
- Scroll down the list to find the Kubernetes content. Download the current CIS Kubernetes Benchmark.
- View the PDF. There are 250+ pages in the document. Instead of reading all of it, find a particular item, such as 1.1.18. Read through the provided information for the item.

CIS Assessment Tool

- Open local browser and navigate to the CIS homepage, https://cisecurity.org. Select the Cybersecurity Tools tab.
- Scroll down and take a look at the options available. On the right of the page you can see a color code for resources that are free, and others are paid.
- Select the CIS-CAT Lite automated assessment tool. We will test Ubuntu, both to ensure we are secure as well as to see a sample of what the assessment does and eventually returns. Fill out the form on the right and submit. This will cause an email to be sent to you.
- Inside the email you will eventually receive you will find the option to download version 3 or version 4. Instead of clicking on the green button, hover with the mouse over version v4 and copy the link. Then log into your exercise node and use the **wget** command to retrieve the file.
- As this manner of download creates a long and difficult file name you can use the mv command and tab to rename it to something easier, like CIS-Cat.zip.
- To extract the files we may first have to install the unzip command. *sudo apt-get update ; sudo apt-get install unzip*
- Use the newly installed command to extract all the files. After extraction change into the newly created directory. *unzip CIS-Cat.zip*.
- The assessment tool requires JAVA. Install the software then set the JAVA_PATH variable. *sudo apt-get install openjdk-11-jdk -y && export JAVA_PATH=/usr/lib/jvm/java-11-openjdk-amd64/bin/*
- Run the Assessor-CLI.sh script without any options. You should see some warnings and a text graphic, followed by help information. Among that information note the levels of verbosity as well as the -i option to run an interactive assessment. Use the sudo command as the tool requires root ability. *sudo bash Assessor-CLI.sh*
- Run the program again, this time pass the -i option. When the Select Content prompt appears enter the number 5, to assess Ubuntu. *sudo bash Assessor-CLI.sh -i*
- You should then see options about what level of testing you want to do. Chose option 1. There will be a lot of output following. Take a moment to scan through the hundreds of tests. Some will pass, some will fail. At the end of the output you should see total assessment time and a location for the HTML report.